UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,567	01/05/2004	Chanwoo Kim	4475-032498	3573

28289 7590 11/10/2009

THE WEBB LAW FIRM, P.C.
700 KOPPERS BUILDING
436 SEVENTH AVENUE
PITTSBURGH, PA 15219

EXAMINER	
SHEPPERD, ERIC W	
ART UNIT	PAPER NUMBER
2453	

MAIL DATE	DELIVERY MODE
11/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/751,567	KIM, CHANWOO	
	Examiner	Art Unit	
	ERIC W. SHEPPERD	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 July 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3 are pending.

Response to Amendment

2. In response the amendment filed 07/09/2009: Applicant has submitted replacement drawings, and the corresponding objections are withdrawn. Applicant has amended the specification, and the corresponding objections have been withdrawn. Applicant has amended the claims, and some of the corresponding 35 USC § 112 rejections have been withdrawn.

3. The amendment filed 07/09/2009 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Claim 1 lines 37-38 "exceeds a reference number set within a predefined time out period". Claim 1 line 40 "the IP collision decision module determines IP collisions for all IPs" (emphasis added).

Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

4. Applicant's arguments filed 07/09/2009 have been fully considered but they are not persuasive. The rejection of claims 1-3 has been updated to reflect amended claims (*see below*).

Claim Rejections - 35 USC § 112

5. Claims 1-3 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. As to claim 1, lines 15-16 the limitation "determines if a filtered ARP packet is collided IP packets" is grammatically incorrect. For purposes of applying prior art the limitation has been construed as "determines if a filtered ARP packet is a collided IP packet".

7. As to claim 1, line 16 the limitation "if it is" is vague and indefinite. For purposes of applying prior art the limitation has been construed as "if the filtered ARP packet is a collided IP packet".

8. As to claim 1, line 22 the limitation "the access" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "access".

9. As to claim 1, line 28 the limitation "periodically saves it" is vague and indefinite. For the purposes of applying prior art it has been construed as "periodically saves the detected collided IP data".

10. As to claim 1, lines 29-30 in the phrase "the detected collided IP data to another system and notifies an administrator of it" the limitation "it" lacks proper antecedent basis. For purposes of applying prior art the limitation has been construed as "the detected collided IP data".

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al (US 7,124,197 B2), in view of Matsukawa (US 2001/0017857 A1), in view of Thiele et al (US 2005/0050353 A1).

13. As to claim 1, Ocepek substantially discloses a system for detection and blocking of IP collisions, comprising:

a packet capture driver module that collects all packets detected in a network ("Network Interface driver 132 operates network interface 140 in 'promiscuous' mode" Ocepek Column 9 lines 31-32);

an ARP packet filtering module that filters only ARP packets among the packets being captured from the packet capture driver module ("Detection routing 114 determines if the frame is a "who-has" ARP request" Ocepek column 9 lines 36-37 the *routine singling out ARP requests is a form of filtering*);

an IP collision decision module that determines if a filtered packet is a collided IP packet or not ("Upon receipt of the corresponding ARP replies … access monitoring routine determines whether allowed client devices … respond with the same allowed client Mac address 166 found in allowed client list 150" Ocepek column 10 lines 55-60)

and, if the filtered ARP packet is a collided IP packet, transmits the results to a listing module ("For every MAC address that is not the same or not received, access monitoring routine 120 instructs list control 126 to delete the record from the allowed client list 150" Ocepek column 10 lines 60-62);

an access blocking decision module that notifies an access status when the filtered ARP packet is an ARP request packet and the ARP request packet is included in an access blocking policy list ("Access blocking routine 122 queries list control 126 for records in blocked client list 152" Ocepek column 11 lines 1-2);

an access blocking module that, depending on the access blocking decision module's decision to block access on a particular packet, blocks network access by transmitting an ARP respond packet in response to the particular packet ("For every IP address returned by list control 126 access monitoring routine 120 generates a blocking ARP reply 34 and instructs network interface driver 132 to transmit the blocking ARP replies 34 onto network 12" Ocepek column 11 lines 4-7);

a data storage module that stores information set to operate the collided IP detection system ("Operating system and the routines of security module 106 are run on CPU 134 of security device 10 and may be loaded from secondary memory 136" Ocepek column 8 lines 9-11), a detected collided IP list ("Blocked list" Fig. 8, item 152 *is part of* "Data Structure", item 128 *which is part of the* "Security Module", item 106), and a newly detected host's IP and MAC address lists ("Restricted List" Fig. 8, item 152 *is part of* "Data Structure", item 128 *which is part of the* "Security Module", item 106 *and* "Detection routine then instructs list control to add the IP address of the unknown client

device to restricted client list" column 9 lines 46-48);

a search list logging and saving module that internally lists detected collided IP data and periodically saves it in a storage medium ("Management of data structure 128 is controlled by list control 126" Ocepek column 8 lines 28-29); and

for each IP (Ocepek column 9 lines 31-35 *all clients are detected*) confirms the ARP packet as IP collision and adds the ARP packet to a list ("access blocking routine 122 determines whether the client device 24 at the queried IP address responds with the same MAC address as the blocked client MAC address 170 found in blocked client list 152" Ocepek column 11 lines 15-18 *if the address is the same blocking continues, it only stops if the address checked is different*)

Ocepek fails to explicitly disclose transmitting the detected collided IP data to another system and notifying an administrator of the detected collided IP data, and wherein the IP collision decision module determines if the number of ARP respond packets occurring exceeds a reference number set within a predefined time out period, and confirms the ARP packet as IP collision if the number of ARP respond packets occurring exceeds the set reference number.

Matsukawa describes a method for detecting duplicate IP addresses using ARP request and respond packets.

With this in mind, Matsukawa discloses wherein the IP collision decision module determines if the number of ARP respond packets occurring exceeds a reference number ("Two or More" branch of "Number of ARP Reply Packets Received" Matsukawa Fig. 2 item B6) set within a predefined time out period ("A wait state for an

ARP reply packet as a response to the ARP request packet is set with an appropriate period of time" Matsukawa [0039] lines 1-3), and confirms the ARP packet as IP collision if the number of ARP respond packets occurring exceeds the set reference number ("Determine Detection of IP Address Duplication" Fig. 2, item B8). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the duplication detection method of Matsukawa with the method of Ocepek as it provides a substitute method with predictable results, of checking if an IP address is being duplicated.

The above combined art of Ocepek and Matsukawa fail to explicitly disclose transmitting the detected collided IP data to another system and notifying an administrator of the detected collided IP data

Thiele describes a method for detecting unknown computer attacks, by checking packets for known/unknown exploits.

With this in mind, Thiele discloses transmitting the detected collided IP data to another system and notifying an administrator of the detected collided IP data ("program 30 sends the current packet or the entire TCP sequence of related packets which includes the entire TCP sequence of related packets which includes the current packet, as an alert to SOC 40 for further analysis as a fully filtered, new exploit candidate" Thiele [0027] lines 64-67 *SOC is a* "Security Operations Center" Fig. 1, item 40). It would have been obvious at the time the invention was made to a person of ordinary skill in the art to which said subject matter pertains to combine the method of Thiele with the method of Ocepek and Matsukawa as would increase network security by providing

the ability to identify new computer viruses, worms, exploitation code or other unwanted intrusions (Thiele [0011] lines 2-3).

14. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al (US 7,124,197 B2), in view of Matsukawa (US 2001/0017857 A1), in view of Henry et al (US 7,093,030 B1).

15. As to claim 2, Ocepek substantially discloses a method of detecting IP collisions using an IP collision detection system between a client and a server, comprising the steps of:

(a) collecting all packets created by accessing a network ("Network Interface driver 132 operates network interface 140 in 'promiscuous' mode" Ocepek Column 9 lines 31-32);

(b) filtering only ARP packets among the collected packets ("Detection routing 114 determines if the frame is a 'who-has' ARP request" Ocepek column 9 lines 36-37 the *routine singling out ARP requests is a form of filtering*);

(c) determining whether a filtered ARP packet is an ARP request packet or an ARP respond packet ("Upon receipt of the corresponding ARP replies via network interface driver 132" column 10 lines 55-56);

(d) adding a MAC address to a list by IP address if the filtered ARP packet is an ARP request packet (Ocepek Fig. 10-12 *lists of IP and MAC addresses*);

executing on all IPs to detect IP collisions for all IPs (Ocepek column 9 lines 31-

35 *all clients are detected*).

Ocepek fails to disclose (e) incrementing a count by one for each ARP respond packet; (f) determining if the number of ARP respond packets occurring by IP exceeds a reference number set within a predefined time out period, and if the number of ARP respond packets occurring by IP exceeds the set reference number, confirming the ARP packet as IP collision and adding the ARP packet to a list; and resetting an IP counter if the number of the ARP respond packets occurring is less than the set reference.

Matsukawa discloses (e) incrementing a count by one for each ARP respond packet ("the number of ARP reply packets received is checked" Matsukawa [0043] lines 2-3 *and* "If it is determined that two or more ARP reply packets are received" Matsukawa [0045] lines 1-2 *each reply packet gets counted*); (f) determining if the number of the ARP respond packets occurring exceeds a reference number ("Two or More" Matsukawa Fig. 2 item B6) set within a predefined time out period ("A wait state for an ARP reply packet as a response to the ARP request packet is set with an appropriate period of time" Matsukawa [0039] lines 1-3), and if the number of ARP respond packets occurring by IP exceeds the set reference number ("Two or More" branch of "Number of ARP Reply Packets Received" Matsukawa Fig. 2 item B6), confirming the ARP packet as IP collision ("Determine Detection of IP Address Duplication" Fig. 2, item B8) and adding the ARP packet to a list ("Each input IP address is managed in the form of a list in a database in correspondence with one of the following assigned states: ... "IP address duplication" Matsukawa [0056] lines 1-5); and determining if the number of the ARP respond packets occurring is less than the set

frequency ("One" branch of "Number of ARP Reply Packets Received" Matsukawa Fig. 2 item B6). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the duplication detection method of Matsukawa with the method of Ocepek as it provides a substitute method with predictable results, of checking if an IP address is being duplicated.

The above combined art fails to explicitly disclose resetting a counter.

Henry describes a network interface driver for processing internetworking protocols for a host computer, independently from the host operating system.

With this in mind, Henry discloses resetting a counter ("Reset Monitoring Counter to Zero" Henry Fig. 5, item 530 *counter is reset after receiving ARP reply* "ARP-Reply Packet Received?" Fig. 5, item 519). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the network interface driver of Henry with the method of the above combined art as it would facilitate quicker upgrading of internetworking functions by removing the need to directly modify the IP stack that is built into an operating system (Henry column 1 lines 20-22).

16. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ocepek et al (US 7,124,197 B2), in view of Matsukawa (US 2001/0017857 A1), in view of Henry et al (US 7,093,030 B1), in view of Chandra et al (US 7,366,113 B1).

17. As to claim 3, the above combined art of Ocepek, Matsukawa and Henry substantially disclose the invention as claimed as described in claim 2, including further comprising the steps of:

confirming if an IP address or IP or MAC are included in a block policy list if the filtered ARP packet is an ARP request packet ("the source IP address of the ARP request is compared to the IP addresses found in access status lists 146" Ocepek column 9 lines 37-40);

broadcasting an ARP respond packet to block access, wherein the network access is blocked ("blocking ARP replies 34 are broadcast to all devices on network 12" Ocepek column 7 lines 21-22).

The above combined art fails to explicitly disclose unicasting an ARP respond packet prior to broadcasting.

Chandra describes a discovery process for mapping all the links in an ad hoc network, including a panic mode for a node that is unable to directly communicate with its known neighboring nodes.

With this in mind, Chandra discloses unicasting an ARP respond packet prior to broadcasting ("If the node is unable to get a unicast message delivered ... it might still be able to get its message sent upstream if it broadcasts it" Chandra column 16 lines 30-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to combine the process of Chandra with the method of the above combined art as it increases the ability for nodes of a network to pass messages to each other, strengthening the

reliability of the network.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Kwan (US 7,562,390 B1) is relevant to ARP collecting.

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ERIC W. SHEPPERD whose telephone number is (571)270-5654. The examiner can normally be reached on Monday - Thursday, Alt. Friday, 7:30 AM - 5PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on (571)272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/E. W. S./
Examiner, Art Unit 2453

/Liangche A. Wang/
Primary Examiner, Art Unit 2453